



## FortiAnalyzer™

Centralized logging, analysis and reporting



### Comprehensive Visualization of Your Network

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

### Key Features & Benefits

Graphical Summary Reports	Provides network-wide reporting of events, activities and trends occurring on FortiGate® and third party devices.
Network Event Correlation	Allows IT administrators to quickly identify and react to network security threats across the network.
Scalable Performance and Capacity	FortiAnalyzer family models support thousands of FortiGate and FortiClient™ agents, and can dynamically scale storage based on retention/compliance requirements.
Centralized Logging of Multiple Record Types	Including traffic activity, system events, viruses, attacks, Web filtering events, and email filtering.
Seamless Integration with the Fortinet Product Portfolio	Tight integration allows FortiAnalyzer resources to be managed from FortiGate or FortiManager™ user interfaces.
Choice of Standalone, Collector or Analyzer mode	Can be deployed as an individual unit or optimized for a specific operation (such as Store & Forward or Analytics).
Virtual and Physical Appliance Form Factors	Available for VMware and multiple hardware appliance form factors. Also available as an integrated solution with FortiManager.

### Fortinet's Versatile Management Solution

Networks are constantly evolving due to threats, organizational growth or new regulatory/business requirements. Traditional analysis products focus on recording and identifying company-wide threats through logging, analysis and reporting over time.

FortiAnalyzer offers enterprise class features to identify these threats, but also provides flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements while aggregating logs in a hierarchical, tiered logging topology.

Key tenets of Fortinet's management versatility:

- Diversity of form factors
- Architectural flexibility
- Highly customizable
- Simple licensing



#### FortiCare

Worldwide 24x7 Support  
support.fortinet.com



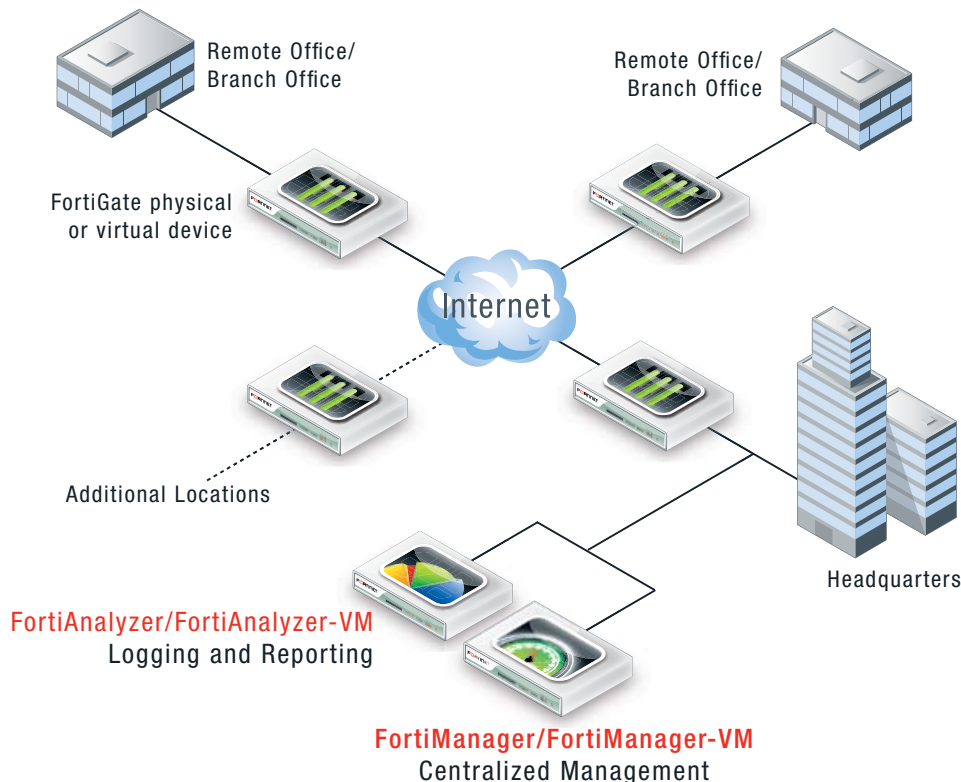
#### FortiGuard

Threat Research & Response  
www.fortiguards.com

# HIGHLIGHTS

## Reporting and Visualization Tools

- **UTM & Traffic Summary Reports**  
Regularly analyze the security profile and traffic/bandwidth patterns with a new consolidated UTM/Traffic report.
- **Per User Summary Reports**  
Instant visibility into the bandwidth usage, web browsing habits and application usage of “top talkers” on the network.
- **Built-in Report Templates**  
Utilize or modify the PDF templates to display colorful, comprehensive, graphical network security and usage reports.
- **Real-Time Monitor**  
Dashboard-style monitor gives IT administrators unprecedented insight into real-time bandwidth & application usage.
- **Scheduling & Report Calendar**  
Automatically generate reports at predetermined times or in an ad-hoc fashion using specific time periods and/or other filters of your choosing.
- **Import/Export Templates**  
After building a report, export and modify the configuration on another FortiAnalyzer or different ADOM.
- **Report “Building Blocks”**  
Create new datasets (SQL queries), charts and layouts specific to your requirements that can be reused within multiple reports.



## Log Viewer

- View logs in real-time or historical
- Select from traffic, event and UTM logs
- Browse by device, ADOM or in aggregate
- Log filtering and search capabilities
- Granular inspection with the log details pane
- Intuitive icons for countries, applications, etc.

## DLP Archiving

- Investigate DLP content archives
- Supported archive types include: email, HTTP, FTP, IM
- View archive text or download files

## Alerting

- Comprehensive alert builder
- Trigger off of severity levels, specific events, actions and destinations
- Set varying thresholds by number of events within a certain timeframe
- View or search through historical alerts
- Notify via email/SNMP or raise a syslog event

## Better with FortiManager

- Enterprise-class device management
- Familiar GUI for full network control
- Available as integrated solution with FortiAnalyzer

## FortiAnalyzer Supported Devices

- FortiGate Multi-Threat Security Systems
- FortiMail Messaging Security Systems
- FortiClient Endpoint Security Suite
- FortiWeb Web Application Security
- FortiManager Centralized Management
- Any Syslog-Compatible Device

SPECIFICATIONS

	FORTIANALYZER-200D	FORTIANALYZER-300D	FORTIANALYZER-1000C	FORTIANALYZER-2000B	FORTIANALYZER-3000D	FORTIANALYZER-4000B
Capacity and Performance						
GB/Day of Logs	5	15	25	75	150	150
Sessions/Day	18 M	55 M	85 M	260 M	520 M	520 M
Maximum Log Rate (Standalone Mode)	350	625	1,000	3,000	6,000	6,000
Average Retention at 5 GB Logs/Day	3 months	1 year	2 years	3 years	4 years	6 years
Devices/ADOMs/VDOMs Supported (Max)	150	200	2,000	2,000	2,000	2,000
Hardware Specification						
Security Hardened Platform	Yes	Yes	Yes	Yes	Yes	Yes
Total Interfaces	4x GbE	4x GbE	4x GbE	6x GbE	4x GbE, 2x GbE SFP	2x GbE, 2x GbE SFP
Number of Hard Drives	1	2	1 (4 Drives Max)	2 (6 Drives Max)	8	6 (24 Drives Max)
Removable Hard Drives	No	No	Yes	Yes	Yes	Yes
Storage Capacity	1 x 1 TB	2 x 2 TB (4 TB Max)	1 x 2 TB (8 TB Max)	2 x 2 TB (12 TB Max)	8 x 2 TB (16 TB Max)	6 x 1 TB (24 TB Max)
RAID Storage Management	No	Yes (0, 1)	No (Yes with Optional Drives 0, 1, 10)	Yes (0, 1, 5, 10, 50)	Yes (0, 1, 5, 10, 50, 60)	Yes (0, 1, 5, 6, 10, 50, 60)
Redundant Hot Swap Power Supplies	No	No	No	Yes	Yes	Yes
Dimensions						
Height x Width x Length (in)	1.8 x 17.1 x 13.9 in	1.7 x 17.1 x 14.3 in	1.7 x 17.1 x 24.7 in	3.4 x 17.4 x 26.8 in	3.4 x 20 x 29.7 in	6.9 x 19.1 x 27.2 in
Height x Width x Length (cm)	4.5 x 43.3 x 35.2 cm	4.4 x 43.5 x 36.4 cm	4.3 x 43.4 x 62.7 cm	8.6 x 44.3 x 68.1 cm	8.7 x 48.2 x 75.5 cm	17.5 x 48.5 x 69.0 cm
Weight	13.4 lbs (6.1 kg)	15.9 lbs (7.2 kg)	35.0 lbs (15.9 kg)	63 lbs (28.6 kg)	71.5 lbs (32.5 kg)	94.5 lbs (43 kg)
Form Factor	Rack mount, 1 RU	Rack mount, 1 RU	Rack mount, 1 RU	Rack mount, 2 RU)	Rack mount, 2 RU	Rack mount, 3 RU
Environment						
AC Power Supply	100–240 VAC, 50–60 Hz, 6 Amp Max	100–240 VAC, 50–60 Hz, 4 Amp Max	100–240 VAC, 50–60 Hz, 7.5 Amp Max	100–240 VAC, 50–60 Hz, 9 Amp Max	100–240 VAC, 50–60 Hz, 9 Amp Max	100–240 VAC, 50–60 Hz, 11.5 Amp Max
Power Consumption (AVG)	60 W	162 W	189 W	200 W	393 W	420 W for 6 HDD
Heat Dissipation	205 BTU/h	666 BTU/h	643.6 BTU/h	519 BTU/h	2153 BTU/h	1433.7 BTU/h (6 drives) 2034.6 BTU/h (12 drives)
Operating Temperature	32 to 104 deg F (0 to 40 deg C)	50 to 95 deg F (10 to 35 deg C)	32 to 95 deg F (0 to 35 deg C)	50 to 95 deg F (10 to 35 deg C)	50 to 95 deg F (10 to 35 deg C)	32 to 104 deg F (0 to 40 deg C)
Storage Temperature	-13 to 158 deg F (-35 to 70 deg C)	-40 to 158 deg F (-40 to 70 deg C)	-40 to 149 deg F (-40 to 65 deg C)	-40 to 149 deg F (-40 to 65 deg C)	-40 to 149 deg F (-40 to 65 deg C)	-13 to 158 deg F (-25 to 70 deg C)
Humidity	5 to 95% non-condensing	8 to 90% non-condensing	5 to 95% non-condensing	5 to 95% non-condensing	20 to 90% non-condensing	5 to 95% non-condensing
Compliance						
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/ cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/ cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, UL/cUL, CB, NOM, GOST	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, UL/cUL, CB

	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Capacity and Performance					
GB/Day of Logs	1 incl.	+1	+5	+25	+100
Sessions/Day	3.5 M	3.5 M	18 M	85 M	360 M
Device Quota	200 GB	+200 GB	+1 TB	+8 TB	+16 TB
Devices/ADOMs/VDOMs Supported (Max)	10,000	10,000	10,000	10,000	10,000
Hypervisor Support	VMware ESXi / ESX 4.0 / 4.1 / 5.0 / 5.1				
Network Interface Support (Min / Max)	1 / 4				
vCPUs (Min / Max)	1 / Unlimited				
Memory Support (Min / Max)	1 GB / Unlimited				



GLOBAL HEADQUARTERS	EMEA SALES OFFICE	APAC SALES OFFICE	LATIN AMERICA SALES OFFICE
Fortinet Inc. 1090 Kifer Road Sunnyvale, CA 94086 United States Tel: +1.408.235.7700 Fax: +1.408.235.7737	120 rue Albert Caquot 06560, Sophia Antipolis, France Tel: +33.4.8987.0510 Fax: +33.4.8987.0501	300 Beach Road #20-01 The Concourse Singapore 199555 Tel: +65.6513.3730 Fax: +65.6223.6784	Prol. Paseo de la Reforma 115 Int. 702 Col. Lomas de Santa Fe, C.P. 01219 Del. Alvaro Obregón México D.F. Tel: 011-52-(55) 5524-8480

Copyright © 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. FAZ-DAT-R13-201305